Como a Inngage trata dados pessoais

ARTIGO · PÚBLICO

SUMÁRIO

1. Nosso papel: operadora
2. Que dados passam pela Inngage
3. Para que usamos
4. Onde os dados ficam e transferência internacional
5. Como protegemos
6. Com quem compartilhamos (suboperadores)
7. Direitos dos titulares
8. Retenção e eliminação
9. Incidentes
10. Transparência e auditoria
11. Documentos
12. Contato e atualizações

A Inngage opera uma plataforma de dados de clientes e engajamento multicanal — o **Inngage Context Cloud** — usada por empresas de varejo e e-commerce para se comunicar com seus próprios clientes. Esta página explica, em linguagem direta, que dados passam pela Inngage, com que papel, onde ficam, quem acessa e como são protegidos. Ela resume os compromissos formalizados no nosso Acordo de Tratamento de Dados (DPA) e vale para toda a operação.

Encarregado (DPO): Raphael Senna e Silva — dpo@inngage.com.br

1. Nosso papel: operadora

Em quase todo o tratamento, a Inngage é **operadora** nos termos da LGPD: os dados pertencem aos nossos clientes (os **controladores**), que decidem o que coletar, com qual base

legal e para quê. Nós tratamos esses dados exclusivamente para prestar o serviço contratado e seguindo as instruções do cliente.

Na prática, isso significa que **nunca**:

- usamos dados de um cliente para beneficiar outro cliente;
- vendemos, cedemos ou compartilhamos dados com terceiros fora da prestação do serviço;
- usamos dados pessoais de clientes para treinar modelos de IA;
- fazemos benchmark ou enriquecimento cruzado entre contas.

Somos **controladores** apenas dos dados de nossos próprios contatos comerciais, leads, colaboradores e dos usuários que acessam o painel da plataforma.

2. Que dados passam pela Inngage

Categoria	Exemplos	Origem
Identificadores	ID de usuário definido pelo cliente, e-mail, telefone, token de dispositivo	SDK, API, importação
Perfil	campos cadastrais e customizados definidos pelo cliente	API, importação, integrações (e-commerce, ERP, CRM)
Dispositivo e sessão	modelo, sistema operacional, idioma, IP, localização aproximada ou geofence (quando habilitada pelo cliente)	SDK
Comportamento e transações	navegação, eventos no app/site, compras, carrinho	SDK, API, integrações
Interações com mensagens	entrega, abertura, clique, resposta, descadastro	plataforma

Fora do escopo: dados sensíveis (saúde, biometria, origem racial, religião, opinião política, vida sexual) e dados de menores de idade. Nossos contratos vedam o envio desses dados.

3. Para que usamos

Somente para executar o serviço: unificar perfis e eventos (CDP), segmentar audiências, orquestrar jornadas e enviar mensagens pelos canais contratados — push (mobile e web), in-app, e-mail, SMS, WhatsApp e RCS — e medir o resultado. Cada conta é logicamente isolada das demais em todas as camadas da plataforma.

4. Onde os dados ficam e transferência internacional

A plataforma roda no **Google Cloud Platform**, por padrão na **região US-Central (Estados Unidos)**, com banco de dados próprio e replicado dentro desse ambiente. Para clientes que exigem residência de dados no país — setor financeiro, por exemplo — oferecemos **implantação dedicada na região Brasil (São Paulo, `southamerica-east1`)**, prevista em contrato; nesse caso os dados da plataforma permanecem no Brasil e a transferência internacional se limita aos canais de entrega listados na seção 6. Imagens de mensagens e envio de e-mail usam a **Amazon Web Services**.

Isso configura **transferência internacional de dados** (art. 33 da LGPD). A Inngage mantém, nos contratos com seus provedores de infraestrutura, as salvaguardas exigidas pela LGPD e pela ANPD para transferências internacionais, e declara esse fato no DPA de cada cliente. Os canais de envio (WhatsApp, RCS, SMS, e-mail, push) envolvem provedores no exterior listados na seção 6.

5. Como protegemos

Controle	O que fazemos
Segregação	Cada cliente tem seus dados isolados por identificador de conta e aplicativo em todas as camadas
Criptografia	TLS em todas as interfaces (SDK, API, painel); criptografia em repouso no armazenamento e nos backups, pelos controles nativos do provedor de nuvem
Acesso ao painel	Usuário individual, perfis de permissão por conta e por aplicativo, **MFA** via WhatsApp no login
Acesso interno	Equipe interna com acesso nomeado, menor privilégio, logs de ações; acesso a banco e infraestrutura restrito a usuários técnicos específicos e revisado periodicamente
Testes de segurança	**Pentests automatizados semanais** e **pentests mensais** revisados com o time e com terceiros
Backup e continuidade	Backup diário do banco de dados, réplicas ativas; retenção de backup de 72 horas
Desenvolvimento	Ambientes separados, dados fictícios em desenvolvimento e teste, revisão de código, dependências atualizadas
Segredos	Credenciais e chaves em cofre gerenciado, rotação em caso de suspeita
Infraestrutura e rede	Provedores de nuvem certificados ISO 27001, SOC 1/SOC 2 e PCI DSS; firewall de borda com detecção de intrusão; acesso administrativo por VPN; monitoramento contínuo dos sistemas
Pessoas	NDA e Código de Conduta para colaboradores e prestadores; revogação de acesso no desligamento
Incidentes	Política de Resposta a Incidentes com prazos definidos e Encarregado nomeado

6. Com quem compartilhamos (suboperadores)

Usamos fornecedores para hospedar a plataforma e entregar mensagens. Todos são vinculados por contrato a obrigações de proteção de dados equivalentes às nossas, e só recebem o necessário à sua função.

Fornecedor	Função	Dados	País
Google Cloud Platform	Hospedagem e processamento	Todos	EUA (US-Central) por padrão; Brasil (São Paulo) em implantação dedicada
Amazon Web Services (S3, CloudFront, SES)	Imagens de mensagens; envio de e-mail	Imagens; e-mail e conteúdo	Exterior
Google FCM / Apple APNs	Entrega de push	Token de dispositivo, conteúdo	EUA
Gupshup	Envio de WhatsApp	Telefone, conteúdo, eventos de entrega	Exterior
Pingoo	Envio de RCS	Telefone, conteúdo, eventos	Brasil
Sophialis / ExpertSender	Envio de e-mail (broker)	E-mail, conteúdo, eventos	Exterior
TOPOL	Editor de e-mail	Templates (sem dado pessoal)	Exterior
OpenAI / Anthropic	Recursos de IA da plataforma e da operação	Dados enviados pela funcionalidade de IA acionada pelo cliente; sem uso para treinamento de modelos	EUA

Alterações nessa lista são comunicadas aos clientes com 15 dias de antecedência, com direito de oposição. A lista vigente é sempre esta página.

7. Direitos dos titulares

Se você é usuário de um aplicativo ou site que usa a Inngage, o controlador dos seus dados é a empresa dona desse aplicativo. Exerça seus direitos (acesso, correção, exclusão, portabilidade, oposição, revogação de consentimento) diretamente com ela. A plataforma oferece ao cliente as funcionalidades para atender esses pedidos, e nós damos suporte técnico em até 5 dias úteis.

Se um pedido chegar diretamente à Inngage, encaminhamos ao controlador no mesmo dia. Pedidos relativos a dados dos quais a Inngage é controladora (contatos comerciais, usuários do painel) são atendidos por dpo@inngage.com.br em até 15 dias.

Para descadastro de mensagens, use o link ou comando de opt-out presente na própria mensagem — ele é processado imediatamente na plataforma.

8. Retenção e eliminação

- Durante o contrato, o cliente define a retenção dos seus dados por meio das configurações e integrações da plataforma.
- Ao encerrar o contrato, o cliente tem **30 dias** para exportar seus dados; depois disso, eliminamos os dados pessoais dos sistemas produtivos em até **60 dias** e dos backups no ciclo de rotação (72 horas).
- Dados anonimizados ou agregados podem ser mantidos para estatística e melhoria do serviço.
- Retenções exigidas por lei ou para exercício regular de direitos são mantidas pelo prazo legal, com acesso restrito.

9. Incidentes

Qualquer incidente que afete dados pessoais de um cliente é comunicado a ele em até **72 horas** após o conhecimento, com natureza dos dados, titulares envolvidos, riscos e medidas adotadas. A decisão de notificar a ANPD e os titulares é do controlador; a Inngage fornece todas as informações e o suporte necessários. Nosso processo completo está na Política de Resposta a Incidentes.

10. Transparência e auditoria

Disponibilizamos aos clientes, mediante solicitação, documentação de conformidade — políticas, descrição de controles e relatórios de testes de segurança — e aceitamos auditoria anual nos termos do DPA. Cooperamos com fiscalizações da ANPD.

11. Documentos

- Acordo de Tratamento de Dados (DPA) — modelo
- Política de Resposta a Incidentes
- Código de Conduta e Segurança da Informação
- Documentos sob NDA (relatórios de pentest, detalhamento de controles): solicite a dpo@inngage.com.br

12. Contato e atualizações

Dúvidas, pedidos de titulares e denúncias: **dpo@inngage.com.br**. Esta página é revisada ao menos uma vez por ano e sempre que houver mudança relevante; o histórico de versões fica ao final.

Versão	Data	Alteração
1.0	26/10/2026	Publicação inicial